PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/32

A1

(11) International Publication Number: **WO 98/51037**

(43) International Publication Date: 12 November 1998 (12.11.98)

(21) International Application Number: PCT/CA98/00417

(22) International Filing Date: 4 May 1998 (04.05.98)

(30) Priority Data:
9709136.7 2 May 1997 (02.05.97) GB

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard West, Mississauga, Ontario L5R 3L7 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: VANSTONE, Scott, A. [CA/CA]; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA). JOHNSON, Donald, B. [US/US]; 7684 Knightshayes Drive, Manassas, VA 20111 (US).

(74) Agents: PILLAY, Kevin et al.; Orange & Associates, Toronto Dominion Bank Tower, Suite 3600, Toronto–Dominion Centre, Toronto, Ontario M5K 1H6 (CA).

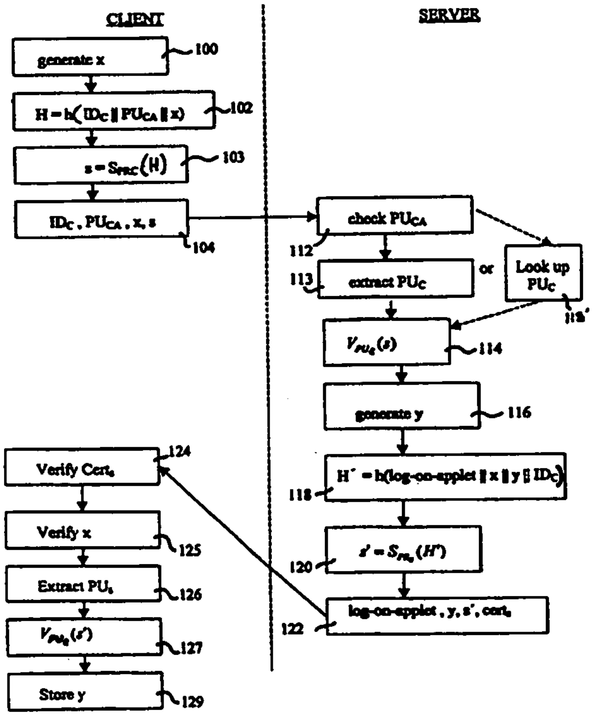
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A LOG–ON VERIFICATION PROTOCOL

(57) Abstract

A method and apparatus for authenticating a pair of correspondents C, S to permit exchange of information therebetween in an information exchange session. The correspondent C having log on applets and the correspondent having means for processing applets. The method comprising the steps of: the first correspondent C transmitting to the second correspondent S a first unique information, the second correspondent S verifying the identity of C and generating a second unique information; transmitting to C the first and second unique information; the C verifying the first unique information to thereby establish currency of the session; the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request; the second correspondent S transmitting to C the requested information along with said second and third unique information; said C verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session; said C repeating steps the above steps for each additional information requested by C.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

A LOG-ON VERIFICATION PROTOCOL

This invention relates to a protocol for the secure receipt and transmission of data between a pair of correspondents and in particular for the secure receipt of data by a client in a client-server environment.

BACKGROUND OF THE INVENTION

With the advent of the Internet and the proliferation of Internet users along with the dramatic increase in data baud rates, there has been a move to distributed computing. For example, in the windows environment, a browser may be used to access a website and download a HTML page. Within the page might be included a program applet much like an image that is contained within the page. The applet's code is transferred from the server to the client system and executed by the client's computer. There are also instances where software or program applets are provided from a server to a client.

In the cases where the client does not trust the server a protocol has to be implemented whereby the client is able to authenticate the server. Or more generally where the client does not know the server since the server will serve any client, i.e. any requester is potentially valid as far as the client is concerned. Furthermore the applets received from the server include in some instances a log-on applet received from the server. Thus there exists a need for a log-on applet authentication protocol.

SUMMARY OF THE INVENTION

This invention seeks to provide a solution to the problem of server verification by a client.

According to an aspect of this invention there is provided a method of authenticating pair of correspondents C, S to permit exchange of information there between in an information exchange session, the method comprising the steps of:

a) the first correspondent C transmitting to the second correspondent S a first unique information,

b) the second correspondent S verifying the identity of C and generating a second unique information;

c) transmitting to C the first and second unique information;

d) the C verifying the first unique information to thereby establish currency of the session;

e) the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request;

f) the second correspondent S transmitting to C the requested information along with said second and third unique information;

g) said c verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

h) said C repeating steps e) to g) for each additional information requested by C.

Also, this aspect of the invention provides for apparatus for carrying out the method. Such an apparatus can comprise any computational apparatus such as a suitably programmed computer.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other advantages of the present invention will become more apparent from the following discussion of preferred embodiments of the invention which are described by way of example only and with reference to the accompanying drawings in which like elements have been assigned like reference numerals and wherein:

Figure 1 is a schematic diagram of a client server configuration;
Figure 2 is a schematic diagram showing server authentication; and
Figure 3 is a schematic diagram showing applet authentication.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Referring to figure 1, a typical arrangement in which the protocol may be implemented is shown generally numeral 10. A client 12 includes a hardware token 14 and connects via a suitable communication channel 16 to a server 18. The hardware token 14 may be PIN activated and includes a root certifying authority (CA) public key, PU_{CA}, a client private key, PR_C,.and an ECDSA signing software. It may be noted that the hardware token may also be mimicked or implemented in software.

In addition to the hardware token the client has stored therein an identification of the client, ID_C, wherein some cases the ID could be the certificate of the client containing the public key PU_C of the client. Alternatively the certificate may contain only the identity ID_C of the client. This identity may then be used as an index into a look-up table of public keys stored in the server. Additionally, the client includes a hash function such as SHA-1, an elliptic curve DSA (ECDSA) verification software, and optionally MQV key exchange algorithm software and a DES or TDES encryption algorithms which are used to encrypt and/or authenticate applets from the server.

The server includes log-on applets, crypto software and other applets. The server also includes a private key PR_S and a certificate $CERT_S$ which includes its public key PU_S. Optionally the server may also include a database of client public keys indexed by a client identification.

Referring now to figure 2, when the client 12 wishes to requests an applet from a server for the first time, the client first authenticates the server by generating a random number x 100, preferably on the hardware token 14. A counter or a time stamp or the like may generate the value x. A hash H on the concatenation of the client identification ID_c, the root public key and x is computed 102. A signature s of the hash H is calculated using the client private key PR_C 103. The client then sends a request 104 containing ID_C, PU_{CA}, x, s to the server 18. The client to indicate the currency of the transaction or session uses the value x.

The server then checks that root certifying authority public key PU_{CA} is correct 112. The client public key PU_C is either extracted 113 from the certificate or a lookup 113' is performed in the server database. The signature s is then verified 114 using PU_C.

The server then generates a random number y 116 and computes the hash H' 118 on the concatenated message of the log of the applet, x, y and ID_C. A signature s' on the hash H' is computed using the server private key PR_S 120. A response 122 is sent to the client and includes the log-on applet, y, s' and the server's certificate

$CERT_S$. Once the client receives this information it verifies the validity of $CERT_S$ 124. The client also verifies x 125, which was sent back with the message from the server and thus indicating the currency of the session. The public key of the server PU_S is extracted from the certificate 126 and used to verify the signature s′ 127. This then verifies the server to the client. The value y is also extracted saved by the client 129 to be used in later transactions.

Turning to figure 3, once the client has verified the server it may then request an appropriate applet by first generating a random number *z* 210. A request 214 is then sent to the server which includes an identification of the appropriate applet 212 and the random number *z*. The server then computes a hash H″ on the concatenation of the applet, *y*, *z* and ID_C 216. The server then computes a signature s″ 218 on the hash H″ using the private key of the server PR_C . Both the applet and the signature s″ are then sent to the client 220. The client verifies the signature 222 using the server public key and once verified may safely use the applet. The value $_y$ is also verified 223 to establish currency of the session Th value $_z$ is also checked 224o make sure it is current. If the client requires more applets, steps 210 to 224 are repeated for a given session. When a new session is resumed the client may re-authenticate the server as set out in figure 2.

While the invention has been described in connection with a specific embodiment thereof and in a specific use, various modifications thereof will occur to those skilled in the art without departing from the spirit of the invention.

The terms and expressions which have been employed in the specification are used as terms of description and not of limitations, there is no intention in the use of such terms and expressions to exclude any equivalents of the features shown and described or portions thereof, but it is recognized that various modifications are possible within the scope of the invention.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of authenticating pair of correspondents C, S to permit exchange of information therebetween in an information exchange session, the method comprising the steps of:

a) the first correspondent C transmitting to the second correspondent S a first unique information,

b) the second correspondent S verifying the identity of C and generating a second unique information;

c) transmitting to C the first and second unique information;

d) the C verifying the first unique information to thereby establish currency of the session;

e) the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request;

f) the second correspondent S transmitting to C the requested information along with said second and third unique information;

g) said c verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

h) said C repeating steps e) to g) for each additional information requested by C.

2. A method as defined in claim 1, said unique information being a random number x.

3. A method as defined in claim 2, said correspondent C including a hardware token for generating said random number.

4. A data communication system for providing exchange of authenticated information between a pair of correspondents C, S in an information exchange session, said system comprising:

a) said first correspondent C including a hardware token having a public key, a private key and ECDSA program; said program for

i) transmitting to the second correspondent S a first unique information,

ii) the second correspondent S verifying the identity of C and generating a second unique information;

iii) transmitting to C the first and second unique information;

iv) the correspondent C verifying the first unique information to thereby establish currency of the session;

v) the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request;

vi) the second correspondent S transmitting to C the requested information along with said second and third unique information;

vii) said correspondent c verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

viii said C repeating steps v) to vii) for each additional information requested by C.

5. A system for authenticating pair of correspondents C, S to permit exchange of information therebetween in an information exchange session, the system comprising:

a) means for transmitting by the first correspondent C to the second correspondent S a first unique information,

b) means for verifying the identity of C by the second correspondent S and generating a second unique information;

c) means for transmitting to C the first and second unique information;

d) means for verifying the first unique information by the C to thereby establish currency of the session;

e) means for generating a third unique information and transmitting the third unique information to the S along with an information request;

f) means for transmitting to C the requested information along with said second and third unique information;

g) means for verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

h) means for successively requesting additional information by said correspondent C.

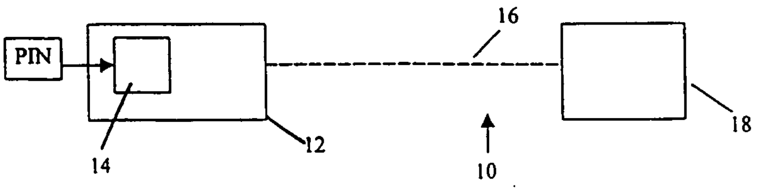


Figure 1

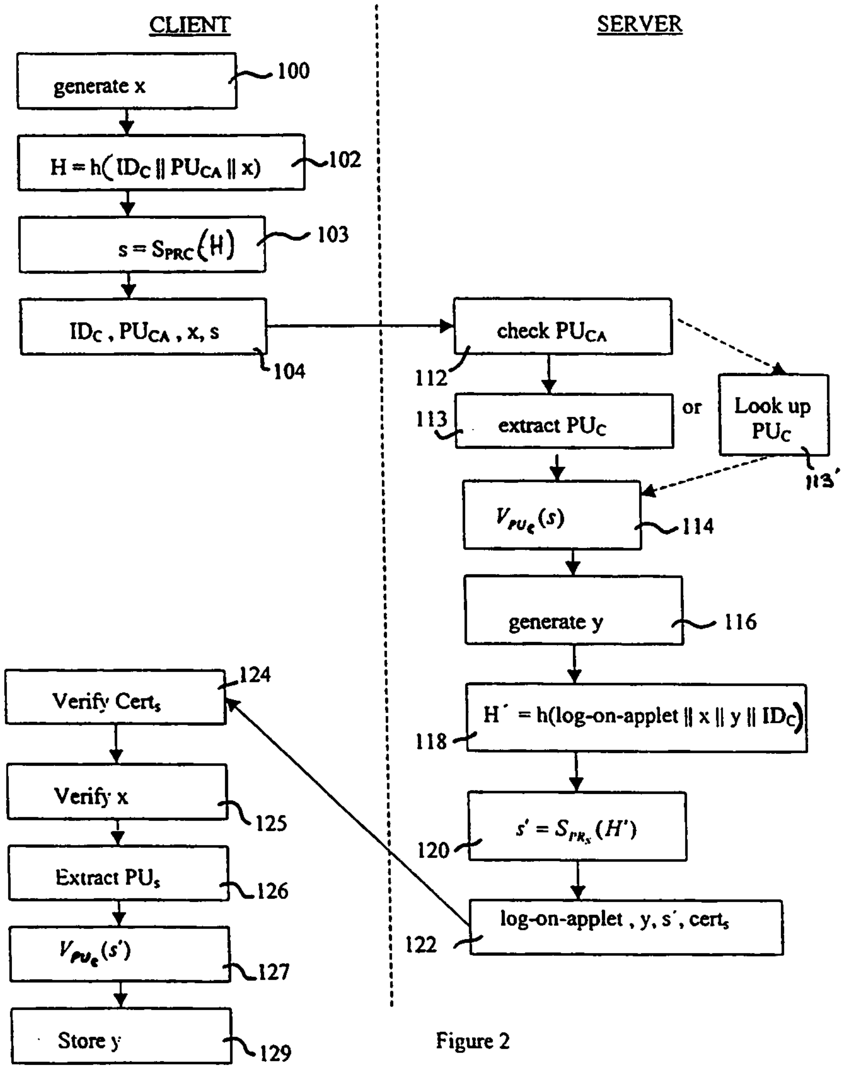


Figure 2

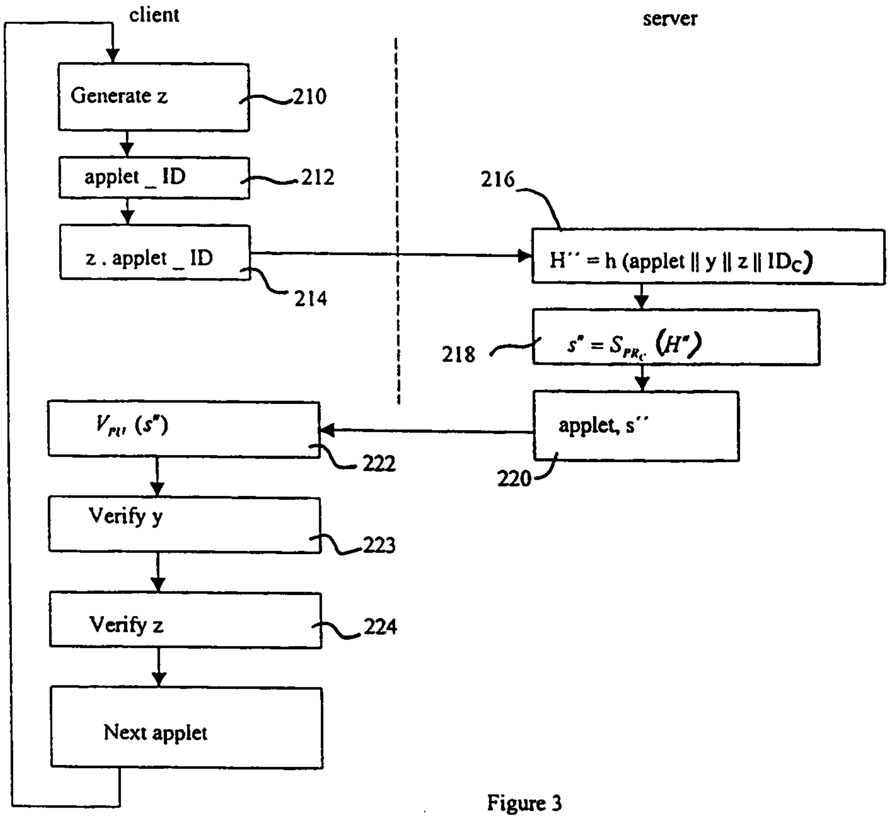

client
server
Generate z
210
applet _ ID
212
z . applet _ ID
214
216
H'' = h (applet || y || z || IDc)
218
$s'' = S_{PR_C}(H'')$
applet, s''
220
$V_{PU}(s'')$
222
Verify y
223
Verify z
224
Next applet

Figure 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 98/00417

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	I'ANSON C ET AL: "SECURITY DEFECTS IN CCITT RECOMMENDATION X.509 -THE DIRECTORY AUTHENTICATION FRAMEWORK" COMPUTER COMMUNICATIONS REVIEW, vol. 20, no. 2, 1 April 1990, pages 30-34, XP000133725 NEW YORK (US) see page 31, paragraph 3.1 - page 32, line 3 see page 32, paragraph 4.1 - page 33, line 21 --- -/--	1,2,5

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 23 September 1998	Date of mailing of the international search report 29/09/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G

1

INTERNATIONAL SEARCH REPORT

I national Application No
PCT/CA 98/00417

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropnate, of the relevant passages	Relevant to claim No.
A	MIYAJI A: "ELLIPTIC CURVES OVER FP SUITABLE FOR CRYPTOSYSTEMS" ADVANCES IN CRYPTOLOGY - AUSCRPYT '92 GOLD COAST, QUEENSLAND, DEC. 13 - 16, 1992, no. CONF. 3, 13 December 1992, pages 479-491, XP000470467 BERLIN (DE) see page 479, line 1 - line 13 ---	1,4
A	PIL JOONG LEE: "SECURE USER ACCESS CONTROL FOR PUBLIC NETWORKS" ADVANCES IN CRYPTOLOGY - AUSCRYPT, SYDNEY, JAN. 8 - 11, 1990, no. CONF. 1, 8 January 1990, pages 46-57, XP000145201 SEBERRY J;PIEPRZYK J BERLIN (DE) see page 51, line 18 - page 52, last line ---	1,4
A	US 5 434 918 A (KUNG ET AL.) 18 July 1995 see the whole document -----	1,5

INTERNATIONAL SEARCH REPORT

Information on patent family members

It ational Application No
PCT/CA 98/00417

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5434918 A	18-07-1995	AU 676107 B	27-02-1997
		AU 1261595 A	03-07-1995
		CA 2153879 A	22-06-1995
		EP 0683907 A	29-11-1995
		JP 8502847 T	26-03-1996
		NO 953143 A	10-08-1995
		WO 9516947 A	22-06-1995